Sharing the Knowledge: Government-Private Sector Partnerships to Enhance Information Security

INTRODUCTION

> *There are two reasons to be especially concerned about information warfare. First, there is the growing dependence on worldwide information infrastructures through telecommunications and computer networks. Second, both nations and terrorist organizations can with relative ease acquire the techniques to penetrate information systems.*[1]

Rising Threats, Vulnerabilities, and Risks

The U.S. defense establishment is driven by and dependent upon advanced information technologies. A quick glance at joint and service doctrine, operational concepts, organizations, and modern weapon systems shows the degree to which the military depends upon information systems. While information technologies have revolutionized the U.S. military, they have also brought with them new threats, vulnerabilities and risks.

Threats to and vulnerabilities in the defense information infrastructure (DII) and national information infrastructure (NII) are rising and demand the attention of the military. Structural factors not likely to disappear contribute to the increasing threats and vulnerabilities. Since it is impossible to completely defend or harden either the DII or NII against electronic intrusions or cyber attacks, the military must develop means to reduce the attendant risks to acceptable levels. A comprehensive risk reduction and management program has numerous dimensions, including employing intrusion detection technologies, training system operators and users, isolating critical network elements from the NII during attacks, and increasing network diversity. However, perhaps the most important element in a risk reduction program entails sharing electronic intrusion and attack information with network owners and operators—in other words, partnering and sharing sensitive information with the private sector.

Information sharing between the military and private sector is crucial to any defense against information attacks. Presidential policy clearly calls out the need for public-private partnership with a particular emphasis on information sharing to defend against cyber attacks.[2] However, establishing a partnership and meaningful information flows is not easy due to substantial barriers, such as private sector concerns over possible releases of sensitive business information under Freedom of Information Act requests and potential government antitrust actions. Nevertheless, examples of successful public-private partnerships that exchange sensitive information abound, including the National Coordination Center for Telecommunications (NCC), the Network Security Information Exchanges (NSIEs), and the CERT® Coordination Center (CERT/CC).

Information sharing based on trusted relationships is vital to any defense against electronic intrusions and information attacks—without it, deterring and blunting information attacks is substantially more complicated. Given the military's critical reliance upon information systems and assets owned and operated by the private sector, the defense establishment should seek to establish a close information sharing partnership with the private sector.

Objectives and Scope

This study examines issues associated with information sharing, explores existing successful models of information sharing, and recommends policy options to improve the interactions between the military—and, more generally, the government—and private sector. The focus throughout is on the barriers to information sharing and potential remedies. The private sector has expressed its view that several of the barriers to sharing, particularly FOIA and antitrust, are show-stoppers. If the government and private sector cannot jointly arrive at solutions to these barriers, an open and voluntary information sharing mechanism will be difficult if not impossible to establish.

Although the primary interest of this analysis is protecting those information infrastructure elements crucial to military operations, it is impossible to develop a military-private sector information-sharing facility in isolation from the rest of government. For example, the intelligence community develops indications and warnings essential to understanding the threat environment. The legal community provides a framework and context for actions the military can lawfully undertake to protect information assets. Law enforcement has the lead investigative role in the aftermath of electronic intrusions or attacks. Finally, the policy community develops overall guidance for the nation's information infrastructure protection program. The scope of military information assurance activities and responsibilities are tightly linked to these communities, so any military-private sector information-sharing program must be developed in the broader context of a government-private sector partnership. For this reason, the ensuing analysis will examine the more general problem of government-private sector information sharing, even though the primary concern rests with the protection of those information assets upon which the military relies.

Organization

The paper first examines the general case for information sharing. It commences by exploring the threat, vulnerability, risk, military, and business environments, each of which has been profoundly influenced by the information revolution. Structural factors in each environment drive an overarching need for risk reduction and management. After surveying means of reducing risks, the focus narrows to key aspects of information sharing with particular attention on creating a business case for exchanging information. Unless both the government and private sector can show a return on investment for the costs entailed with information exchanges, a sharing mechanism will not be viable.

The paper then addresses information sharing barriers. These barriers are associated with concerns over release of material under Freedom of Information Act requests, antitrust actions, protection of business confidential and other private material, liability due to shared information, release of national security material, and additional burdens arising from cooperation with law enforcement agencies. Given the existence of forums that regularly exchange sensitive information, the government and private sector can likely overcome these barriers.

Next, the paper examines four such forums and draws upon their experiences for insights into potential means of overcoming barriers. The chapter explores in some detail the NCC, NSIEs, CERT/CC, and the Global Aviation Information Network (GAIN). The purpose is not to provide a detailed compendium of information-sharing entities, but rather to draw out key lessons learned from these four forums.

Finally, the paper proposes policy options to assist the establishment of a government-private sector information-sharing mechanism. The paper concludes with a summary of the principle findings of this study.

TOWARD A CASE FOR INFORMATION SHARING

> *Although it is a considerable challenge to stay ahead of intruders in an environment characterized by tremendous growth in complexity, vulnerabilities, and potential threats, significant progress has been made in a number of areas to*

> *help organizations manage the risks to their information systems and networks. Comprehensive information system security programs can be used to deter, detect, mitigate, prevent, and respond to electronic intrusion attacks. However, to justify the expenditure of resources for such a program, awareness and information sharing are required to foster understanding and stimulate sufficient interest throughout the public and private sectors.*[3]

As information networks and systems become ever more complex and vital to combat and day-to-day peacetime operations, the threats to these systems have grown increasingly sophisticated. The popular and technical press regularly report on vulnerabilities in information systems and the latest hacking exploits. The trends of increasing threats, growing vulnerabilities, greater military reliance upon the information infrastructure, and the changing business environment are driven by a number of structural factors that are not likely to disappear in the future. These trends mandate that the government and private sector jointly take steps to reduce risks to acceptable or manageable levels. One essential element of a risk management program is information sharing between the government and private sector on threats, vulnerabilities, intrusions, best practices, and other security measures.

This section examines the case for information sharing between the government and private sector. It begins with a survey of several environments: the threat, risk, and vulnerability environments in which DoD operates its information systems; the military environment that is fundamentally dependent upon information superiority; and the rapidly evolving business environment that introduces additional pressures and stresses on the information infrastructure. Under an overarching goal of risk reduction, the section next explores several means of lowering risks confronting information systems and networks. The focus then narrows to information sharing with a view toward types of information that could be shared to reduce information system risks. Different users of shared information, such as system administrators and policymakers, have different information requirements that may present barriers to sharing in their own right. Finally, the section develops a rationale for information sharing, including an examination of factors generally considered in business cases for information sharing.

Environments

Examining and understanding the environments in which military information systems operate is essential before developing a case for information sharing. These environments are rapidly evolving and driven by underlying structural factors that are not likely to disappear.

Threats. It is widely acknowledged that the threats to information systems are growing and will continue to do so in the future. The Office of the Manager, National Communications System (OMNCS), noted that the overall threat to the public switched network (PSN) rose from 1993 to 1995.[4] More recently, OMNCS noted that "virtually all requirements for [national security/ emergency preparedness] telecommunications and information systems within the United States are supported by the [public network], which has been the target of electronic intrusion attacks."[5] OMNCS asserted that electronic intrusions in telecommunication networks, information systems, and interconnected infrastructures will remain a serious threat in the foreseeable future.[6]

Several statistics illuminate the magnitude of the threats to military information systems. In a widely reported analysis, the Defense Information Systems Agency (DISA) estimated in 1995 that DoD computers were intruded upon perhaps as many as 200,000 times.[7] The rate of cyber events in DoD's information infrastructure continues to rise: currently, 80-100 events are detected daily, of which about 10 require detailed investigations. More than 80 counter-intelligence cases involving cyber events are open, with an additional 15-20 opened each month.[8] A substantial number of countries are developing information warfare capabilities and doctrines.[9] Given the number of foreign nations with information warfare capabilities, the sophistication of software programming capabilities in other nations, and the ubiquity of the Internet, the Joint Staff asserted that the threat to information systems must be given much consideration.[10] Finally, CERT/CC has handled a rapidly rising number of incidents since its inception in 1988, with nearly 4500 events reported in the first half of 1999 alone.[11]

A number of factors contribute to the growing threat to the information infrastructure. First, hacking tools have become increasingly sophisticated and easy to use. Tools and techniques are frequently posted to web sites or bulletin boards, thereby effectively sharing the skills and knowledge required to attack or intrude upon information systems. The sophistication, ease of use, and widespread availability of such tools place substantial power in the hands of the user: even today's novice can inflict considerable damage with a few mouse clicks.

Second, technology sources contribute to the potential threat to information systems. An increasing amount of software and software components is written overseas, which increases the potential for the insertion of backdoors or other malicious code by economic competitors or foreign intelligence services.[12] Similarly, malicious code could be inserted in chips, components, or systems manufactured overseas. Detection of malicious code is not easy, particularly given the large size of modern software packages.[13] This problem has received increased attention due to the volume of Year 2000 (Y2K) software remediation performed by foreign companies.[14]

Third, the principle actors contributing to the threat have constantly evolved. The Defense Science Board Task Force on Information Warfare-Defense examined the actors, the threats they posed, and their likely evolution by 2005.[15] Of particular concern is the projected evolution towards increasingly malevolent and consequently more dangerous actors. Equally worrisome, OMNCS reported that the motives and characteristics of the actors have changed:

- Hackers appear to be more motivated by greed and malice than intellectual curiosity;
- Terrorist organizations are increasingly recruiting hackers and privileged insiders;
- Criminal organizations consider information systems to be lucrative targets for fraud, theft of proprietary information and intellectual property, and theft of funds;
- Over 23 countries are collecting economic intelligence on the United States, with electronic intrusion being a principal means of intelligence gathering; and
- A number of countries are developing information warfare and electronic intrusion and espionage capabilities, including Russia, China, South Korea, Cuba, Japan, France, Germany, Iraq, Israel, and Bulgaria.[16]

Vulnerabilities. Vulnerabilities in the information infrastructure have likewise been widely discussed and analyzed. Recent exercises and real-world events (such as Eligible Receiver, Solar Sunrise, and the attacks against federal agency web sites in 1999[17]) illustrate weaknesses in the information infrastructure and point to the need for concerted action.

A number of structural factors contribute to the growing vulnerabilities in the information infrastructure. First, the Defense Department has increased its use of COTS systems in recent years. Purchase and deployment of COTS software and hardware frequently makes good business sense. Yet despite the advantages of COTS items, there are associated risks and security issues. Increased COTS use can lead to system standardization and loss of diversity. With decreased diversity, vulnerabilities, and security weaknesses in specific products become "standardized" and well-known, leading to a greater proportion of systems at risk to intrusions.

Second, intrinsic characteristics of software and the software development process lead to other information system vulnerabilities. As software grows in size and complexity, it becomes physically impossible to comprehensively test it under all possible operating conditions and states. Further, it is exceedingly difficult to locate embedded malicious code or backdoors in programs. Finally, software developers frequently fail to include security as an integral part of the design process, often adding security features after the fact only if there is sufficient demand.

Third, information networks are frequently unbounded and not secure by nature.[18] Unbounded networks, such as the Internet and PSN, exhibit several characteristics including:

- Large numbers of access points and collocated critical assets;
- Increased number of service providers with implicit trusted relationships among their networks; and
- Large numbers of users and processes with access privileges.

Given the complexity and characteristics of unbounded networks, it is impossible to comprehensively ascertain network operating conditions or analyze them. Massive connectivity and network "growth by accretion" can unintentionally introduce vulnerabilities that go unrecognized until exploited.[19] As the Defense Science Board noted, the economy and military are built on a technology base that is impossible to understand in fine detail or control.[20]

Finally, DoD's increased dependence on information networks introduces its own vulnerabilities. Day-to-day business practices within the department are inextricably linked to computer networks. The DII is pervasively linked to the NII and global information infrastructure (GII), allowing attacks to originate from any point on the globe. While it may at first appear desirable to disconnect DoD's information networks from the Internet, this solution is impractical given the tight couplings among the DII, NII and GII. DoD depends extensively and perhaps critically upon commercial networks, a situation unlikely to change in the future.

Risks. The United States has fortunately not experienced a widespread, debilitating attack on or disruption of its information infrastructure. The Defense Science Board assessed the likelihood of a severe attack on the U.S. before 2005 as low, given the difficulty in planning and predicting the intended results of a strategic attack.[21] Recently, the President's National Security Telecommunications Advisory Committee (NSTAC) concluded that a widespread outage of the national telecommunications network was unlikely.[22] NSTAC defined a widespread outage as:

> …a sustained interruption of telecommunications service that will have strategic significance to government, industry, and the general public. Such an outage would likely affect the telecommunications service in at least one region of the country including at least one major metropolitan area. It would involve multiple carriers, affecting both long distance and local service, and significantly degrade the ability of other essential infrastructures to function. Such an outage would have an impact on the availability and integrity of telecommunications service for at least a significant portion of a business day.[23]

NSTAC considered a variety of mechanisms that could lead to a widespread outage, including software problems, SONET operations control, common channel signaling gateway screening, physical design, sabotage, and the introduction of new technologies or services. Significantly, NSTAC assessed the likelihood of a widespread outage resulting from sabotage as remote, as it would require attacks on multiple facilities and carriers and require a substantial degree of coordination.[24] Despite its assessed low probability of a widespread, sustained outage, NSTAC noted that the societal—and, by extension, national and economic security—implications of such an outage were high enough to merit consideration.[25]

In this light, it is important to consider the risks to the DII in addition to threats and vulnerabilities. In the simplest sense, risk is a function of threats and vulnerabilities—a vulnerability with no associated threat may pose little if any risk. Given current threat and vulnerability trends, the potential risks to the DII are increasing and will continue to do so. Since it is impossible to totally eliminate vulnerabilities or threats, the military must instead take proactive measures to reduce risks to acceptable levels. Joint Publication 3-13, *Joint Doctrine for Information Operations*, directs all DoD elements to "adopt a risk management approach to the protection of their information, information systems, and information-based processes based on potential vulnerability to [information operations]."[26]

Finally, even if the military were able to completely secure its own information infrastructure and assets, a substantial residual risk would remain. The military relies upon the nation's critical infrastructures for its peacetime and wartime missions.[27] In most cases, infrastructures require information and communications networks (the NII) for operations and maintenance functions. To the degree that the NII can be attacked or disrupted, infrastructures dependent upon the NII are vulnerable to disruptions as well. Given the military's reliance upon these infrastructures for its operations, it too depends upon the integrity and security of the NII. Consequently, even if the military were able to completely protect its own information and communication assets from attack, it would still be indirectly—and critically—vulnerable to electronic intrusions in non-defense information networks and critical infrastructures. Vulnerabilities in and electronic threats to the nation's critical infrastructures, including the NII, therefore are a substantial source of additional risk to the military.

The Military Environment. Military reliance upon information is as old as warfare itself. Yet the explosive growth of information technologies during the past several decades has affected every aspect of the way the U.S. military fights, from weapon systems to operational concepts to organizational structures. As the U.S. military establishment becomes more tightly wedded to advanced information technologies, it must take care to avoid creating an Achilles' heel due to threats to and vulnerabilities in the DII, NII, and GII.

There are no indications that the dramatic changes fueled by the information revolution will slow in the U.S. military. In fact, information operations will become increasingly important in the coming decades. From the conceptual template of Joint Vision 2010 to service and joint doctrine to theoretical constructs, the requirement for information superiority is deeply entrenched and regarded as essential to operations. Joint Vision 2010 states that U.S. forces "**must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.**"[28] Underpinning the vision are advanced information and communications technologies and—critically—information superiority.[29] The vision asserts that future improvements in information technologies promise to significantly affect military operations by enabling "dominant battlespace awareness" and mitigating the effects of fog and friction.

There is likewise universal agreement on the importance of information superiority in Air Force and joint doctrine. Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine*, lists information superiority as one of six Air Force core competencies:

> Dominating the information spectrum is as critical to conflict now as controlling air and space, or as occupying land was in the past, and is seen as an indispensable and synergistic component of air and space power. **Whoever has the best ability to gather, understand, control, and use information has a substantial strategic advantage**…. *One of a commander's primary tasks is to gain and maintain information superiority, with the objective of achieving faster and more effective command and control of assigned forces than the adversary*.[30]

AFDD 2-5, *Information Operations*, notes that gaining and maintaining information superiority is important for all core competencies, and that defensive counterinformation is the Air Force's overall top information warfare priority.[31] Joint Publication 3-13, *Joint Doctrine for Information Operations*, puts further context on the crucial nature of joint information operations in modern combat. The publication recognizes the private sector's key role in information operations.[32]

The importance of information superiority in warfare is brought clearly into focus by the "OODA loop," a theoretical construct proposed by Colonel John Boyd.[33] He postulated that systems continuously cycle through a sequence of observations, orientations, decisions, and actions (OODA). A system observes some event of interest, decides how to resolve a problem posed by the event, and finally acts upon that decision. In military operations, the commander's objective is to "get inside the adversary's OODA loop." He does this by simultaneously destroying the enemy's capability to sense, process, and act on information while preserving his ability to do the same—in short, by gaining and maintaining information superiority. Once reaching this point, the commander can force the enemy to react rather than take the initiative. Boyd's OODA construct is frequently employed in military theoretical writings and doctrine. AFDD 2-5 links information operations directly to the OODA loop, noting that "in the final analysis, *information operations exist to support commanders in determining the situation, assessing threats and risks, and making timely and correct decisions*."[34]

That militaries rely upon information is incontestable; with modern weapons and operational concepts, information superiority takes on a new and expanding role. The U.S. military is tightly coupled to the DII, NII and GII. This deep, structural dependency underscores the necessity of risk management vis-à-vis the information infrastructure.

The Business Environment. The rapid evolution of information technologies has been accompanied by a transformation of the business environment. Some of these changes have profound implications for the security of the DII and NII, and consequently must be included in threat, vulnerability, and risk analyses. Four significant, underlying drivers of the current business environment are the Telecommunications Act of 1996, increased competition, the rush to the marketplace with new products and services, and the difficulty of comprehensive product security testing.

The Telecommunications Act of 1996 fundamentally changed the competitive landscape. Section 215(C) of the Act requires local exchange carriers to provide nondiscriminatory interconnection and unbundled network access to requesting providers at any technically feasible point. This requirement gives rise to important security concerns. The Federal Communications Commission's (FCC) Network

Reliability and Interoperability Council (NRIC), with draft inputs from NSTAC's Network Security Group, identified the following issues:

- Increased number of access points and collocation will likely decrease core infrastructure diversity and increase single points of failure;
- Increased number of interconnected service providers with inferred trust relationships will degrade overall security and network integrity;
- Embedded Operations Channels of advanced Signaling and Transport Protocols give virtually unlimited access to everything and everyone connected to them, given the current state of security standards and practices in such advanced technologies;
- More persons and processes with privileges will present major risk challenges;
- Insecure Internet and Intranet technology used for interconnection access to Network Operations and Signaling Systems will provide unintentional back doors to PSN mission critical systems, protocols and information;
- Perceived lack of Regulatory, Legal, or Competitive motivation to invest in security safeguards will increase risks to the PSN; and
- Lack of requirements, fidelity bonds, background checks, or other fiduciary requirements, given the Communications Assistance for Law Enforcement Act control requirements of Section 229 of the Act, [for persons in key positions within telecommunications providers] will increase risk to the PSN.[35]

Although technology, procedures, and policies may mitigate some of these risks, the potential security issues posed by the Act and the required solutions will become clearer only with time.

Increased competition and competitive pressures likewise present new security challenges. With greater competition and lower rates, information and communications service providers are forced to operate on tighter margins and reduce their costs of doing business. Providers have taken various steps to lower their costs, including:

- Centralizing operations and collocating assets. But, concentrating assets in a few locations provides more lucrative targets to terrorists or other malevolent actors.

- Reducing or eliminating personnel at remote sites. Unattended sites, even if closely monitored, might be easier targets for physical exploitation or destruction.
- Decreasing security programs, particularly if the risks from lower security (and attendant lower operating costs) are deemed acceptable in risk calculations.

Each of these steps brings with it new vulnerabilities that must be factored into risk calculations and risk management programs.

Increased competition pushes companies to “rush” new products and services to the marketplace, often before they are fully tested or evaluated from a security and risk standpoint. Being the first to market has powerful incentives, including the potential expansion of one’s customer base and the possibility of establishing an industry standard. However, the rush to market can introduce unforeseen vulnerabilities or unanticipated and potentially harmful interactions into networks, particularly if testing is incomplete.[36] Finally, security features are frequently not an integral part of the product design process, but are instead “add-ons”—particularly if the market does not provide sufficient demand for such features.

The difficulty of comprehensive product testing prior to market introduction deserves special mention. Exhaustive testing of information systems and components under all possible operating conditions and configurations is impossible, which provides opportunities for flaws or vulnerabilities to pass undetected. The current market practice is to ship products with flaws and follow up with patches as users discover problems. If service providers or network operators are not aware of or do not install patches, then networks and information systems retain the original vulnerabilities. Given the rapid dissemination of vulnerability information and hacking tools designed to exploit these holes, this *modus operandi* creates a significant security issue.

The business environment has characteristics that increase vulnerabilities and raise security concerns. As in the military environment, risk mitigation strategies that incorporate new technologies, procedures, policies, and other measures may indicate a path forward.

The Overarching Objectives: Risk Reduction and Management

Considering the complexity of the DII, NII, and GII, it is clearly impossible to develop a comprehensive security program that protects all infrastructure elements all of the time from every conceivable threat. The cost of developing and deploying a completely hardened information infrastructure would be prohibitive, if such a infrastructure could even be devised.[37] Furthermore, DoD does not have the authority or responsibility to protect a substantial portion of the information infrastructure upon which it relies.[38] A more realistic approach, as described in Joint Publication 3-13, is for the defense establishment to assess the value of the information and information systems necessary for it to fulfill its missions, determine the risks associated with the loss or compromise of the information, and protect the information and systems (for which it has the authority and responsibility to do so) at a level commensurate with the risks. In short, risk analysis, reduction, and management provide the best defense.

Given that there are no silver bullets, a risk management and reduction program should consist of multiple, mutually reinforcing steps. This approach provides a layered defense: a single step might not prevent intrusions, but multiple actions could increase the difficulty of carrying out attacks. A comprehensive program would include the following elements:

- Incorporate advanced technologies, such as intrusion detection systems, firewalls, and resilient and fault tolerant system designs.
- Develop, rigorously enforce, review, and update security policies.
- Develop and share best practices and procedures.
- Train and raise awareness of system operators and users.
- Remove unauthorized "backdoor" connections and isolate networks during attacks.
- Increase the diversity of network elements.

Information sharing is a seventh, crucial element of a risk management program. The remainder of this study will focus on this key dimension of risk management.

Key Aspects of Information Sharing

There is broad, general agreement within the government and private sector that information sharing is an essential part of any program designed to protect the nation's information and communications infrastructures. At the highest policy level, Presidential Decision Directive-63 (PDD-63), *Critical Infrastructure Protection*, directs the government to establish information-sharing mechanisms with the private sector.[39] PDD-63 further encourages the private sector to establish Information Sharing and Analysis Centers (ISACs) to gather, analyze, sanitize, and distribute government and private sector information concerning infrastructure attacks to the appropriate government and private sector entities. The President's Commission on Critical Infrastructure Protection (PCCIP) likewise stressed that information sharing underpins government-private sector partnerships essential for critical infrastructure protection.[40] NSTAC has long argued that information sharing, based on a trusted partnership with the government, is essential.[41] In its risk assessment series, NSTAC pointed out that infrastructure owners and operators in other sectors also view information sharing as a requirement for improved security.[42]

One of the first steps in establishing an information-sharing mechanism is to determine the needs of the various communities. The *types* of required information vary from user to user: senior policymaker needs are not the same as those of system administrators or general users. The *level of detail* required will also depend on the specific user, level in the corporate or government hierarchy, and mission particulars.[43] Information sharing mechanisms must be tailored to the specific participant needs.

To further define information-sharing issues, NSTAC's National Coordination Center for Telecommunications Vision Subgroup sponsored a tabletop exercise in 1997 attended by technical and policy experts from the government and private sector. The exercise revealed that there were no criteria defining the types of information that should be collected, reported, and shared. The following bullets summarize the focuses of each sector, their respective information needs, and the speed at which they desire shared information.[44]

- Private Sector:
  - Focus: generation of revenue and minimization of costs, fraud reduction, protection of proprietary information, maintenance of image, ensuring network integrity and reliability. The private sector places a relatively greater emphasis on detecting intrusions that could jeopardize revenues.
  - Needs: specific threat or vulnerability information so that actions can be taken to avert an intrusion or that a business case for additional security can be built.
  - Speed: varies from company to company. Some companies wanted only information with immediate relevance, whereas others desired comprehensive information on past and current vulnerabilities, threats, best practices, etc.
- Law Enforcement:
  - Focus: prosecution of criminals, preservation of case-sensitive material.

  - Needs: Specific information on perpetrators and particular aspects of the attack, the intent of the attack, and the consequences of or damages due to the attack. Some noted that information at the keystroke-by-keystroke level was essential.
  - Speed: as fast as possible in order to avoid "cold trails."[45]

- Intelligence Community:

  - Focus: identification of threats and protection of sources and methods.
  - Needs: range from broad picture to fine detail. Understanding typical network operating conditions will help detect anomalous behavior or abnormal states.
  - Speed: varies depending upon circumstances and use. For indications and warnings, speed is of the essence. However, when examining the details of a case, the need for accuracy and completeness may take priority over speed.

- National Security/Defense:

  - Focus: maintenance of information superiority, assuring access to and protection of mission critical information and information systems.
  - Needs: range from the broad picture for national command authorities to fine-grained detail necessary to protect specific systems. Information needs vary from tactical to strategic levels; depend on the specific level within a command hierarchy; and differ in peacetime, crises, conflicts, and post-conflict periods.
  - Speed: varies depending upon circumstances and use. Speed requirements are different in peacetime, crises, conflicts, and post-conflict periods.

Defining common reporting criteria that satisfy the needs of all communities, at all levels of each organizational hierarchy, at all times, is challenging. The initial steps are to develop a common understanding of the information needs of each community and criteria that outline the information to be shared. These steps must be done jointly, with all communities participating.

Despite the differences highlighted by the exercise, there are general themes for the types and requisite detail of information that should be shared. A preliminary list of types of information that should be considered for sharing includes information and techniques related to risk management; threat and vulnerability information, particularly specific information that can be acted upon immediately; incident reports, including lessons learned and steps taken to mitigate, prevent, and recover from the incident; and technological developments.

It is instructive to examine incident reporting forms developed by several organizations. CERT/CC requests that computer incident reports include the following information:

- Type of affected machine(s), including IP addresses and hostnames;
- Source of the attack(s), including IP addresses and hostnames; and
- Description of the attack(s), including dates, methods of intrusion, intruder tools involved, software versions and patch levels, intruder tool output, details of vulnerabilities exploited, source of the attacks, and other relevant information.[46]

The CERT/CC vulnerability report form requests the following data:

- Impact of the vulnerability, including how it could be used in an attack scenario;
- Whether or not the vulnerability is currently being exploited;
- Whether an exploitation script is available, and if so, a copy of the script;
- Description of known systems and/or configurations that are vulnerable;
- Known workarounds or fixes; and
- Other pertinent information.[47]

CERT/CC's incident response form for incident response teams is considerably more detailed.[48]

NSTAC's NCC Vision Subgroup developed a similar set of incident reporting information. Any reporting process would have to be capable of handling and protecting classified and proprietary information. Information on attacks on data and control systems managing the data would be of particular interest. Finally, the subgroup stated that "to maximize the overall value of intrusion information, an incident must be evaluated to determine what was done, how it was done, how it might be prevented, and, if possible, why it was done."[49]

Several general observations on government-private sector information-sharing mechanisms are pertinent. First, the government and private sector must jointly design the information-sharing mechanism. Although the government can mandate reporting criteria to the private sector, a jointly designed, built, and staffed mechanism is more likely to obtain critical buy-in and acceptance by industry. Second, developing a trusted relationship between the government and private sector is essential. However, nurturing trust and building a productive relationship takes time. Third, the information sharing must be equitable and provide value added to the government and private sector costs of information sharing. Finally, any hesitancy to share will set back an information-sharing mechanism. Developing a successful information-sharing mechanism will take time and demand considerable effort by all participants.

Factors in the Case for Information Sharing

Industry and the government have the same goal for the information infrastructure: effective, secure, uninterrupted, and reliable operations. However, the private sector is motivated by business concerns and profits, whereas the government is driven by national and economic security concerns. These divergent concerns lead to profoundly different world views and perceptions. Importantly, perceptions affect the level of risk each party is willing to accept and the costs each is willing to bear. Herein lies the fundamental difficulty in establishing an joint government-private sector information-sharing mechanism: determining if the payoffs from information sharing are worth the associated costs in light of perceived threats, vulnerabilities, and risks. The government and private sector must both realize benefits that outweigh the costs.

What are the potential payoffs? Several of the more obvious benefits include:

- Ready access to near real-time intrusion information from multiple networks for analysis and data correlation;
- Better coordination of response and recovery actions, particularly if multiple networks are experiencing simultaneous attacks;
- Greater coordination with appropriate intelligence and law enforcement agencies;
- Creation of a centralized resource for best practices, lessons learned, and other important security information; and
- Increased awareness of information security threats, vulnerabilities, and risks.

Sharing electronic intrusion and attack information, best practices, and lessons learned will improve situation awareness in the government and private sector. Given that intruders can rapidly affect systems in widely spread areas, greater situation awareness could mean the difference between blunting an attack or suffering damages.

Before the private sector is willing to share information with the government, it must be convinced that the threats are real and risks high enough to warrant the costs of sharing information. Many in the private sector argue that although the government has repeatedly stated that a clear and growing threat exists, it has yet to offer specific, concrete threat and vulnerability information upon which individual firms can act to protect their assets.[50] The private sector does not believe it has sufficiently detailed information to build a business case and commit resources for additional security measures, including information sharing.

The government and private sector must both be able to make business cases to justify information sharing. Despite the different perceptions and motivations of the private sector and government, several broad themes are common to their business cases:

- Costs, including time, personnel, resources, and money. Although it may be argued that the government should be willing to make a considerable investment in information sharing given national and economic security implications, federal departments and agencies may have to offset other ongoing programs to fund increased information assurance. In the current tight budget environment, developing the political case to offset established programs for added security measures is difficult, even given Presidential policy (PDD-63).
- Risk. For the private sector, corporate health and survival are paramount. Of key concern is the risk to reputation or customer base, especially if the public perceives that a firm's information networks are untrustworthy. The private sector must be convinced that the government can protect shared information from disclosure—if not, the private sector's potential risks are higher. From the government's perspective, protecting national and economic security is paramount. It will thus weigh risk factors differently and may tend to be more conservative than industry.
- Return on investment. The benefits must outweigh costs and risks if the private sector and government are to exchange information. What is the value added from information sharing? For the private sector, the most likely near-term return will be the perceived value of the government information it receives. For the government, the return will be the increased degree of national and economic security.
- Barriers. Discussed in detail in the next chapter, there are substantial barriers to information sharing that present additional risk. For example, the private sector worries that information sharing may lead to liability issues and possible antitrust action. Barrier "heights" and solutions affect business case calculations.

The bottom line is that the benefits derived from information sharing must exceed the actual, potential, and perceived costs. The private sector desires a trusted environment in which meaningful information sharing can take place without fear of regulation, loss of public confidence, liability, or disclosure of sensitive material.[51] The government similarly seeks a mutually beneficial interaction to improve national and economic security.

What, then, are the steps the government and private sector should undertake to help establish their respective business cases? First, and most importantly, the government and private sector should jointly define the types of information both need and are potentially willing to share. Second, the government should examine means by which it can release sensitive threat and vulnerability information to specific, key elements of the private sector. Any such mechanism must protect sensitive government sources and methods. Incontestable proof of serious, specific threats and vulnerabilities will go a long way towards building solid business cases for information sharing. Third, the private sector should consider the kinds of meaningful information it can share. Fourth, the government and private sector must jointly develop methods to lower the information-sharing barriers and risks associated with sharing. Finally, following a decision to establish an information-sharing partnership, the government and private sector should jointly and equitably design, develop, establish, and operate the sharing mechanism. A government-mandated information-sharing center will not stand; a joint center has the potential to provide tangible benefits for both the government and private sector.

Summary

The United States is fortunate in that it has never suffered an "electronic Pearl Harbor" and that its information infrastructures are highly reliable. However, structural trends in the threat, vulnerability, risk, military, and business environments call for prudent risk reduction and management efforts. Given the military's ever-increasing reliance upon information systems and networks, risk reduction and management is not only prudent but essential.

The military—and more generally the government—cannot by itself assure and protect the nation's critical information and communications infrastructures. Only a government-private sector partnership will achieve the goals of greater information infrastructure security, higher network reliability, and lower risks. A key element in any risk reduction and management program is information sharing between the government and private sector. Real-time, equitable, open sharing can be an enabling factor for intrusion detection and alerting, response planning, and reconstitution efforts. Yet before information sharing becomes a reality, both the government and private sector must develop solid business cases that show value added.

One element of the business case is an examination of barriers to information sharing. These barriers must be lowered to acceptable levels before meaningful sharing will take place. The following section examines the principle barriers and potential remedies.

OVERCOMING THE BARRIERS

> *Sharing of sensitive information is probably one of the most important first steps in building a defensive information warfare capability. There are significant legal, regulatory, competitive and emotional hurdles to overcome; these must be addressed as soon as possible.*[52]

As the Defense Science Board points out in the preceding quote, significant barriers stand in the way of information sharing. Yet, given the necessity of information exchange, the government and private sector have strong incentives to overcome the barriers. Examples abound of other mechanisms or forums in which the government and private sector exchange sensitive material, such as the Centers for

Disease Control, despite similar barriers. These mechanisms offer insights and lessons learned that may be applicable to the present case.

This section examines six principle barriers to information sharing. The barriers arise from concerns over release of sensitive material under Freedom of Information Act requests, antitrust actions, protection of business confidential and other private material, possible liability due to shared information, release of national security material, and additional burdens entailed with cooperating with law enforcement agencies. Existing information-sharing forums provide insights and offer possible solutions for the barriers.

Freedom of Information Act

A fundamental requirement of any information-sharing forum is to protect sensitive material from inadvertent release. In the present case, the private sector desires assurances that the government will protect proprietary and other business confidential material. The private sector is particularly sensitive to information releases under the Freedom of Information Act (FOIA) requests. In fact, the private sector views potential FOIA releases of proprietary and other sensitive material as a "show-stopper" for information exchanges.[53]

The private sector is not convinced that the government can provide adequate protection of sensitive material under present FOIA exemptions and federal statutes. Industry has voiced its fears that releases of sensitive or potentially embarrassing material could lead to loss of consumer confidence, higher intrusion risks, and decreased or lost competitive advantages. Furthermore, a government repository of sensitive information infrastructure material would be a prime target for hostile FOIA requests.[54] Ideally, sensitive government or private sector information would be afforded adequate protection from release under FOIA requests.

However, there are countering viewpoints that argue against strengthening protection of such information from FOIA requests. The Electronic Privacy Information Center (EPIC) takes a stand against further FOIA exemptions for sensitive critical infrastructure material, urging that Congress "ensure that the FOIA [is] not amended in any way that would inhibit the public's right to access unclassified information held by the government, regardless of the information's origin."[55] The argument has also been made that going public with security information would *force* better security and security practices.[56] Such arguments aside, the private sector will resist providing sensitive information if there is risk of disclosure.

The challenge, then, is to determine means to adequately ensure protection of such information from FOIA requests yet still meet the intent of FOIA. Exemptions (b)(3) and (b)(4) provide a starting point. Exemption (b)(3) is the stronger of the two and provides protection for:

> matters that are…(3) specifically exempted from disclosure by statute… provided that such statue (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld.[57]

However, no statute currently exists that applies to information shared to protect information and communication infrastructures (or other critical infrastructures).[58]

Several outstanding issues must be resolved before the government can begin drafting legislation for Exemption (b)(3) coverage. First, the type of information to be afforded protection under the exemption must be explicitly and clearly defined. Too narrow a definition may not provide sufficient coverage, while too broad an exemption may run into difficulty with Congress or privacy organizations. Second, the parties that would have access to the information must be clearly defined. Finally, penalties for disclosure of protected material must be carefully delineated. The private sector is vitally interested in the content of such legislation, and the government would do well to obtain private sector comments during the drafting phases.[59]

The FAA provides a model that yields further insight. Under Public Law 104-264, Congress added 49 U.S.C. Section 40123 that requires the FAA to protect voluntarily provided aviation safety information from public disclosure. The argument advanced is that the public is not deprived of information it could otherwise obtain from the FAA, because the FAA would not otherwise receive this information. However, there is significant public benefit for the FAA to receive this information so that it can prevent further incidents.[60] Under this statute and Exemption (b)(3), voluntarily supplied information is protected from FOIA disclosures.

Exemption (b)(4) protects trade secrets or other confidential commercial or financial information voluntarily submitted by businesses to agencies. The key is that the private sector provides its privileged or business confidential material voluntarily to the government, and the government is precluded from releasing properly exempted information publicly through other channels. This applies to information submitted voluntarily as well as that required by the agency where an authority prescribes criteria for submission. Although this exemption can provide protection, it is not considered to be as strong as Exemption (b)(3).[61] Agencies determine what information receives protection under this exemption, leading to concerns that agencies will neither define exempted material nor apply the exemption uniformly. Furthermore, a “proprietary” marking on a document does not provide an ironclad assurance that Exemption (b)(4) will preclude its disclosure.

The government faces a further dilemma: if it provides a private sector ISAC with information, then that information loses FOIA protection. Given that some sensitive information will need to be broadly available to service providers, but *not* to the general public, the government will need to resolve the loss of FOIA protection. Stripping information of identifiers linking it to a specific firm before release may provide some measure of protection, but still will not resolve the problem of protecting potentially damaging information from general release.

It is crucial that the government resolve the FOIA question with the close participation of the private sector. If this issue cannot be resolved to the satisfaction of both parties, it risks precluding the establishment of a viable information-sharing mechanism.[62]

Antitrust Concerns

The private sector has expressed its concern that an information-sharing mechanism could run afoul of government antitrust or anticompetitive laws, a situation serious enough to be a show-stopper for information exchanges.[63,64] Antitrust laws are designed to:

- Make illegal contracts, combinations, or conspiracies in restraint of trade or commerce; and
- Prohibit actual and attempted monopolization of markets resulting from price fixing, market division, tying arrangements, production limitation, and other unreasonable restraints of trade.[65]

Antitrust concerns arise from the very act of sharing information, so care must be exercised in the design and implementation of procedures and processes used to exchange information.

Antitrust issues come to the fore when one or more companies are excluded from access to material shared among other firms, particularly if the shared information provides a competitive advantage. An excluded company could claim that it is the victim of a boycott or that it has been excluded from an essential facility. In a sense, the situation resembles that of the Prisoner's Dilemma game: it may be in the best interests of all companies to cooperate and share information, or to simply not share anything at all.

The Department of Justice's (DOJ) Antitrust Division and the Federal Trade Commission should play active roles in the design of an information-sharing mechanism. Each can provide guidance on means to avoid anticompetitive behavior and review proposed information exchange procedures and processes. Early involvement of these organizations will go a long way toward reducing private sector concerns.

It appears that the government and private sector can overcome this barrier and avoid anticompetitive behavior. An important step is to engage government organizations, such as DOJ's Antitrust Division and the Federal Trade Commission, for guidance and review of proposed information-sharing concepts. The government should actively engage the private sector to explore antitrust concerns and remedies. A government-private sector conference on antitrust issues associated with information sharing would be an ideal venue to start this process.

Confidential Information and Privacy Issues

A third barrier to information sharing centers on confidential information[66] and privacy issues. Although related to FOIA, protection of business confidential information is a broader issue as the information-sharing mechanism must prevent inadvertent release or abuse of private sector information by *any* means. Safeguarding privacy rights and personal information is also problematic and requires careful consideration.

The private sector needs solid assurances that its confidential material will remain just that: confidential. Legal vehicles such as the Electronic Espionage Act, various protections for trade secrets, and provisions in federal criminal and civil codes that protect information uncovered during court proceedings provide a measure of security for business confidential information. However, much as with FOIA concerns, unless there are strong protective mechanisms in place, including penalties for inadvertent disclosure, the business community will remain reluctant to provide sensitive information to the government.[67]

Similarly, personal privacy and civil liberties are important considerations. The primary question is whether the collection, aggregation, analysis, and warehousing of information will infringe upon personal privacy rights. EPIC asserted that several PCCIP recommendations would provide greater expansions of government authority and new encroachments upon civil liberties.[68] Other privacy advocates have argued that monitoring electronic communications goes far beyond tradition wiretapping. For example, if the government can search computers hooked to the Internet, the situation may be more akin to a search of a residence than a wiretap.[69] The recent sharp criticisms leveled by civil libertarians and members of Congress at the National Security Council's plan for the Federal Intrusion Detection Network (FIDNET) indicate the level of concern associated with electronic privacy issues.[70]

Federal policy on personal privacy rights provides broad guidance for the development of an information sharing mechanism. Office of

Management and Budget (OMB) Circular No. A-130, Management of Information Resources, directs:

> The individual's right to privacy must be protected in Federal Government information activities involving personal information[71]…[agencies shall] consider the effects of their actions on the privacy rights of individuals, and ensure that appropriate legal and technical safeguards are implemented.[72]

PDD-63 directs that "care must be taken to respect privacy rights. Consumers and operators must have confidence that information will be handled accurately, confidentially and reliably."[73] The PCCIP recognized the need to balance employers' needs against personal privacy rights, and recommended that the Attorney General convene a group of legal professionals, labor and management organizations, and privacy advocates to further study this issue.[74] Clearly, an information-sharing activity must protect individual privacy rights and civil liberties, and any proposed sharing mechanism should undergo a detailed, rigorous legal and policy review.

Privacy and confidentiality concerns and policy guidance suggest specific points to consider during the design of a sharing mechanism:

- What is the planned or projected use of the information?
- Exactly what information must be shared?
- What is the minimum information that can be shared yet still accomplish the mission?
- Will the aggregation of large amounts of information threaten privacy rights?
- How should such information be sanitized? Can personal or confidential information be masked or otherwise stripped of personal or corporate identifiers?
- Who will have access to the information?[75]
- What are the specific controls over dissemination of the information?
- Are existing legal mechanisms adequate to safeguard the information? What new legal controls are necessary?

- What are the penalties for inadvertent release or abuse of the information? Are they adequate in the views of government and the private sector?
- Do existing or planned legal controls infringe upon personal rights or civil liberties?

Careful consideration of these questions, in consultation with the private sector and privacy groups, is essential to ensure that the dual purposes of protecting information systems and personal or confidential information are achieved.

Liability Concerns

Liability for information shared—or not shared—is another barrier affecting the government, private sector, and individuals. Liability is a multifaceted issue with distinct but related concerns for all parties engaged in information sharing. In certain circumstances, liability can be limited if care is taken when establishing information-sharing processes.

The government can find itself liable for damages under several circumstances. Legal vehicles establishing an information-sharing facility can affect the degree of government liability.[76] If a legal vehicle explicitly states with whom the government will share information, then other parties cannot sue the government for failure to share with them. On the other hand, if the government does not share information with the listed parties out of negligence, then it is liable for damages. Consequently, the selection criteria that determine those entities to whom the government will provide information are crucial: how broadly will the government share its information, and what access rights do or should other entities have to that information? The government can avoid liability if the legal vehicle states that it does not create a right of action against the government. The legal vehicle is thus a crucial element of the information-sharing process and should be carefully crafted.

Liability issues likewise affect the private sector. Under State tort laws, a company could be liable for financial or other damages if it fails to share information or act upon shared information. Antitrust and anticompetitive laws raise other liability issues. For example, a company could be held liable if by sharing information it negatively affects a competitor's market position.[77] Due diligence and duty are additional aspects that further complicate a company's decision to share information. Consider the following scenarios:

- A firm decides to participate in an information-sharing mechanism. To what extent is it liable for damages for failure to act on information it subsequently receives? And how quickly must the firm act upon the information in order to show due diligence and avoid liability?
- A firm participating in an information-sharing mechanism fails to provide information that would have prevented damages to other companies. For example, an extensive vulnerability analysis reveals vulnerabilities that also affect the information systems of other companies. What is the firm's liability if it does not share this information?
- A company decides that it will not participate in an information-sharing mechanism. What is its liability for damages that could have been avoided if it had information available through the sharing mechanism?
- An information-sharing entity obtains information that could prevent electronic intrusions and damages. What is the extent of the entity's liability or that of its members for not sharing this information with nonmembers?

The pros, cons, and potential liability associated with membership are factors in a company's decision whether it should join an information-sharing entity.

One unknown in the liability equation is the role of insurance companies and auditors. In the future, insurers could provide advantages such as lower rates or better terms to those customers that are members of an information-sharing mechanism. Rates, of course, depend on insurance industry calculations of risks and liabilities associated with membership in an information-sharing entity. The degree to which insurance considerations will drive private sector participation in information-sharing mechanisms is unknown but could be substantial.

A final aspect of liability deals with sanctions for reporting information. If employees risk job sanctions or other punishments, they will not report incidents. Furthermore, sanctions imposed on employees will also ensure that further incidents, vulnerabilities, or other irregularities will go unreported—sanctions "shoot the messenger." In a broader context, there are two groups of "messengers:" individual employees reporting within companies, and the firms themselves reporting to the information-sharing body. Messengers must be free of sanctions if information is to flow freely. The government and private sector would do well to establish an environment in which messengers can report incidents without fear of retribution.

National Security Information

The government holds a substantial body of national security (classified) information that could be invaluable in deterring or thwarting electronic intrusions and information attacks. The government frequently classifies threat, vulnerability, and risk assessments to protect sources and methods or to reduce the possibility of exploitation of vulnerabilities. While the government rightfully has to protect classified information, this material creates several dilemmas. First, should the government release classified material, even if on a one-time only basis, to jump-start an information-sharing entity? The private sector has argued that it needs access to such information to build its business cases. But even one-time clearances are problematic, particularly if they must be broadly granted to garner widespread private sector support for information sharing. Second, should the government release classified material to the private sector on a more regular basis? While the private sector would benefit from and is clearly interested in such material, the intelligence community has to protect its sources and methods. Need-to-know and the breadth of dissemination are key considerations. The government must strike a balance among the reduced risks of information attacks resulting from sharing and acting upon classified information, the increased risks to national security from dissemination of classified material, and the intelligence community's need to protect sources and methods.

As a first step, the government should determine with whom it is in the national interest to share such classified information. Granting security clearances to key private sector personnel will provide access where necessary. However, within individual companies, who needs access to classified information, and at what level of classification? The senior executive management of a firm might need limited access to understand the magnitudes of the threats, vulnerabilities, and risks facing their organization. On the other hand, certain system operators and administrators might require broader access as they directly confront the threat and are the corporate "line of defense." Need-to-know is again paramount.

A frequently suggested solution is that the government sanitize classified information and distribute the derivative products to the private sector. Yet sanitized information may have a lower value due to the loss of important details. Declassifying and sanitizing also take time, which could affect time-critical operations or perishable information. In the absence of private sector personnel with the appropriate clearances, the key is to determine *a priori* what information is essential to share. The government and private sector could jointly design templates for sanitized information that retain sufficient detail and timeliness so as to be useful.

A further problem arises with aggregations of unclassified material. Collections of information may be classified, even if individual records are by themselves unclassified. An information sharing or warehousing activity could conceivably amass enough unclassified information that the aggregate becomes classified. The threshold quantities of material required for an aggregate to be classified are not clear; additionally, thresholds might vary depending upon the specific types of information the aggregates contain. As a result, aggregates require careful handling until specific guidance governing their classification levels is available. In any case, a compilation of such information is a lucrative target for malevolent actors.

Sharing sensitive information with foreign-owned companies raises more issues. Defining what is meant by "foreign-owned" company is increasingly difficult given the globalization of industry, mergers, and acquisitions. Determining what can and should be shared with completely or partially foreign-owned firms remains unresolved. The PCCIP recommended developing guidelines for sharing with foreign firms, and suggested creating a sliding scale for determining foreign ownership and information sensitivity based upon infrastructure sector.[78] It will likely be difficult to develop comprehensive guidelines or sliding scales that are broad enough to apply to all situations yet provide adequate protection for classified information. The solution may reside in examining situations with foreign-owned companies on a case-by-case basis.

The Security Policy Board has examined sharing classified critical infrastructure information with the private sector, a closely related problem to the present case. The Board defined "protectable critical infrastructure information" as:

> [s]hared *Threat*, *Vulnerability*, *and Mitigation Strategy* information pertaining to the telecommunications, energy, banking and finance, transportation, water, and emergency services infrastructures that must be protected against unauthorized disclosure to prevent loss of life, placement of the nation at economic, political, or military disadvantage, or interruption of essential infrastructure services.[79]

The Board proposed protecting such information from FOIA release with Exemption (b)(3), with penalties for unauthorized disclosures and an oversight process. The information would be protected for a fixed period of time with possible extensions. Clearly, legislation to provide FOIA protection for this material would be required. The Board suggested that the government could share classified information by first declassifying it and then immediately labeling it "protectable critical infrastructure information." The information could then be shared in a controlled manner with the private sector without fear of release under FOIA requests. If the government validates this proposal and Congress enacts suitable legislation, it could set a precedent for developing a similar system for information pertaining more specifically to information infrastructure protection.[80]

Overcoming the classified information barrier will probably require a combination of the approaches suggested above. The first step is a careful government-private sector evaluation of the specific information needs of each party. Only then can the government properly weigh the risks associated with releasing classified material, either in sanitized form or to appropriately cleared persons, against the security benefits gained from information sharing.

Law Enforcement Barriers to Sharing

Sharing information with the law enforcement community requires overcoming further barriers. Given law enforcement's role in the broader issue of information system security, we will briefly consider these barriers. Information sharing between military and law enforcement entities should present few problems. However, the private sector has reservations about sharing information with law enforcement.

Evidence handling rules are one source of difficulty.[81] Law enforcement has strict rules regarding evidence in order to preserve its integrity for prosecuting cases. The private sector often does not understand the details of evidence handling. Furthermore, developing this expertise in companies does not come for free: industry incurs costs from training, implementing auditing and control mechanisms, and following proper procedures. These costs may deter the private sector from cooperating with law enforcement authorities.

Other factors militate against providing information to law enforcement. A business may not wish to report an incident if its image might be tarnished. Low penalties for crimes, low conviction rates, and questions surrounding the prosecution of juveniles do not provide strong deterrents to electronic intrusions, particularly when compared to the costs incurred by the private sector when cooperating with law enforcement. The private sector may decide—and has done so in the past—that the costs of cooperation are greater than any derived benefits. Under such circumstances, a company will shun cooperation and absorb its losses from intrusions.

Despite the barriers, OMNCS notes that there is evidence of increasing cooperation and information sharing between the private sector and law enforcement.[82] Commercial use of the Internet provides a powerful financial motivation to report intrusions to law enforcement. This motivation will become stronger as the volume of e-commerce rises. Recent successful suits against spammers provide additional incentives to the private sector. Nevertheless, more needs to be done to improve the laws and prosecute those who break them.

Summary

Substantial barriers to information sharing exist, yet it is crucial that the government and private sector jointly examine and implement means to overcome them. Barriers arising from FOIA and antitrust laws deserve special attention as they are "show-stoppers." Given the numerous forums that successfully share sensitive information, there is reason to be optimistic that the government and private sector can arrive at solutions to the barriers. The next section will examine in some detail four successful forums for useful insights and lessons learned.

INFORMATION-SHARING MODELS

> *We envision the creation of a trusted environment that would allow the government and private sector to share sensitive information openly and voluntarily. Success will depend on the ability to protect as well as disseminate needed information.*[83]

Despite serious impediments to information sharing between government and private sector entities, examples of successful sharing mechanisms abound. For example, the PCCIP identified over 100 information clearinghouses at federal, state, and local governmental levels.[84] NSTAC described in detail 11 different information-sharing organizations specifically oriented to information and communications infrastructures.[85] Given the abundance of such organizations, the question is not *if* the government and private sector can devise an information-sharing mechanism, but rather *what lessons can be learned* *and adapted from existing mechanisms to overcome information-sharing barriers*? What analogies can be drawn for the present case?

Four organizations, three of which are within the information and communications infrastructure, are instructive information-sharing models: the National Coordination Center for Telecommunications, the Network Security Information Exchanges, the CERT® Coordination Center, and the Global Aviation Information Network. The mechanisms each organization employs to overcome information-sharing barriers are of particular interest.

Any information-sharing mechanism is limited by the breadth of its membership and the information that its members share. OMNCS asserts that:

> One criticism often leveled at [information-sharing mechanisms] is that they share little or no information outside their limited membership. This limited sharing is a result of the delicate balance between confidentiality and disclosure that must be maintained for effective sharing of information in this sensitive area. Organizations are willing to discuss details of incidents and protection measures within a limited community defined by common interests and trust. Although others outside the process do not benefit from the information, larger audiences would tend to inhibit disclosure to the point that the real value—the details, the "war stories," the open discussion—would be lost.[86]

Each of the organizations examined below has this limitation, despite the important services each offers to its membership. The objective, however, is to look beyond this limitation (and others) for lessons the government and private sector can apply to a general information sharing entity.

National Coordination Center for Telecommunications

Established on 3 January 1984 in the wake of the AT&T breakup, the NCC is a central, authoritative point of contact for national security/emergency preparedness (NS/EP) telecommunications issues. Its mission is to "ensure that the critical NS/EP telecommunications needs of the Federal Government can be and are met in any emergency or crisis situation."[87] Its functions include performing technical analyses and damage assessments of telecommunications disruptions, developing comprehensive restoration plans, maintaining inventories of resources to restore essential telecommunications, monitoring essential telecommunications facilities, coordinating restoration activities, and coordinating emergency provisioning for new services for NS/EP needs. The NCC originally consisted of representatives of the National Communications System (NCS), 11 companies, and the United States Telephone Association. Today, four government agencies and seven corporations form the NCC's resident membership.

In 1998, NSTAC and the NCC examined adding a new function to share information on electronic intrusions to the NCC charter. After determining that an indications, analysis, and warning (IAW) function fell within the charter's scope, the NCC undertook a pilot IAW project in 1998. Based on the results of the pilot project, which yielded few shared intrusion reports, the NCC and NSTAC are jointly revising reporting criteria and the concept of operations.[88]

Several key lessons from the establishment and operation of the NCC stand out. First, government-industry cooperation has been a hallmark of the NCC since the initial planning phase. Both the Executive Office of the President and NSTAC approved the NCC's functions. The functions in the operational guidelines are joint government-industry undertakings: both parties operate the watch center, assess disruptions and other telecommunications events, exercise, and develop mission support, operational, and other plans.

The second key lesson is that the close government-private sector cooperation the NCC enjoys lies on a solid foundation of trust built by both parties over the past 15 years. Developing the degree of trust among the NCC participants took considerable time and effort. To a large extent, trust grew from personal, daily contacts among the participants over time. If it is to continue its information-sharing operations, the NCC must maintain this high level of trust.

The third lesson concerns protection of proprietary information from FOIA or other unauthorized releases. The NCC *Operational Guidelines* address information sharing, noting that sharing is essential to NCC operations. The *Operational Guidelines* state that "all industry entities represented in the NCC should not employ the NCC as a forum for attempting to obtain proprietary information regarding other NCC industry entities."[89] Noting the exclusion of proprietary information from FOIA requests, the *Operational Guidelines* further direct establishment of procedures for handling proprietary information in order to avoid unauthorized disclosures. Before releasing an incident report to government or industry representatives, a private sector submitter must resolve all concerns regarding proprietary information. If the firm and NCC Manager cannot resolve a dispute over proprietary information, the information reverts to the firm. The internal operating procedures seek to ensure the anonymity of the entity reporting an incident; the reporting firm or agency determines those NCC representatives with whom it wishes to share the incident information.[90] The government and industry designed NCC operating procedures from the onset to protect proprietary and business sensitive material, and the NCC has been successful in doing so.

A fourth lesson comes from the manner by which the government and private sector addressed antitrust issues. The Manager, National

Communications System, consulted extensively with DOJ's Antitrust Division and FCC to avoid potential antitrust issues during the design of the NCC. The Antitrust Division noted that the NCC must not involuntarily disclose proprietary information to competitors, and that voluntary sharing arrangements must not reduce competition.[91,92] It further recommended that the NCC adopt procedures to prevent potentially anticompetitive involuntary information disclosures. Furthermore, DOJ noted that the government, not industry, should limit NCC membership. DOJ recommended that the government design selection criteria to promote as broad an industry participation as possible, with the minimum possible restrictions necessary for mission accomplishment. To this end, the government wrote strict criteria for industry participation into the NCC charter and selected the participating industry members. Based on the selection criteria and initial private sector members chosen by the government, DOJ believed that there would be no antitrust concerns, provided that NCC operations did not of themselves raise any issues.[93] The FCC also reviewed the membership selection criteria and proposed industry members and found no legal or regulatory concerns.[94] The NCC's key actions included early consultations with DOJ and FCC, proper design of industry member selection criteria, and careful selection of industry members.

The NCC is a successful information-sharing entity that offers several key lessons. Trust is essential to the NCC's success, yet it took years for the government and industry members to develop the current high level of trust. Government and industry jointly approved the NCC mission and functions, and today work closely with one another to fulfill the mission. Finally, the government addressed key barriers early in consultation with DOJ and FCC. Several of these themes will reappear in the forums examined below.

Network Security Information Exchanges

The NSIEs grew from National Security Council (NSC) concerns over the growing hacker threat in the early 1990s. The NSC directed the NCS to identify actions to protect NS/EP telecommunications from this threat. The government and private sector finalized the NSIE charters in May 1991, and the NSIEs first met the following month. Their primary mission is to share information on threats, incidents, and vulnerabilities affecting public network software.

There are in reality two NSIEs: one chartered by the government with representatives from 11 agencies, and the other chartered under NSTAC with members from 19 companies. The NSIEs meet jointly, voluntarily share information, and coordinate closely with each other.

The NSIEs have instituted procedures that permit the sharing of sensitive materials including classified information.[95] Each member organization signs a nondisclosure agreement, and all representatives and guests sign personal acknowledgements before attending any meetings. All representatives hold at least secret security clearances which facilities sharing classified information. Perhaps the most interesting feature is a designator system for controlling NSIE information. The most tightly controlled materials are designated N-1 and may only be shared among NSIE representatives. Information designated N-2 may be shared with individuals in NSIE member organizations who have a need-to-know as determined by their NSIE representative. Finally, N-3 materials may be shared beyond NSIE member organizations.

The key points to draw from the NSIEs for the protection of sensitive materials are the use of nondisclosure agreements, the requirement that members hold security clearances, and the internal categorization of materials as N-1, N-2, and N-3.

CERT® Coordination Center

In the aftermath of the Morris worm incident in 1998, the Defense Advanced Research Projects Agency charged the Software Engineering Institute, Carnegie Mellon University, to establish a capability to coordinate communications among experts during computer security incidents and prevent future incidents. The result was CERT (later renamed CERT® Coordination Center), whose mission is "to work with the Internet community in detecting and resolving computer security incidents as well as taking steps to prevent future incidents."[96] CERT/CC focuses on security improvements, survivable network technologies and analysis techniques, incident response, incident and vulnerability analyses, knowledge base development, and courses and seminars to increase security awareness. The center publishes a variety of advisories, incident and vulnerability notes, technical tips, vendor-initiated bulletins, and other security-related materials. While CERT/CC only receives information from those sites that wish to report vulnerabilities or intrusions, it broadly distributes warnings and other information through its web site and publications. CERT/CC will also facilitate coordination with law enforcement authorities when a site specifically requests help.

CERT/CC has built a solid reputation for objectivity and discretion. This reputation is due in no small part to the center's proven ability to keep identities and sensitive information confidential. It keeps all information submitted by sites confidential unless the sites specifically authorize release of the information. CERT/CC strongly recommends the use of encryption and digital signatures to protect submissions. Furthermore, it will not release any vulnerability information unless a patch is available.[97]

Trust is the essential enabler in the successful operation of CERT/CC. The level of trust is evident in reporting statistics compiled by CERT/CC since its inception a decade ago. The center has received 235,000 e-mail messages, 16,200 hotline calls, 17,800 computer security incidents, and more than 1,100 vulnerability reports.[98] Clearly, if CERT/CC did not maintain its high reputation, it would not experience this level of activity.

The principle lessons to draw from CERT/CC are the importance of trust and the requirement to develop procedures to protect confidential information.

Global Aviation Information Network

GAIN is the result of FAA concerns over current aviation accident rates.[99] After falling for years due to improved technologies and procedures, accident rates hit a plateau and remained there for the past 10-15 years. The FAA believes that further reductions are only possible by collecting, analyzing, and sharing accident and incident information. The FAA intends GAIN to develop a sharing and analysis capability that detects emerging issues and disseminates safety information to the worldwide aviation community. The FAA desires to eliminate the “we all knew about that problem” syndrome that often appears in accident investigations.

GAIN is based upon *voluntary* information sharing. It ties diverse data sources from across the aviation community, such as voluntary incident reporting, digital flight data, and air traffic control radar data, with analytic tools such as qualitative risk assessment, data mining and visualization, and statistical methods. However, its proponents expect that little if any raw data will be shared; rather, the resultant analyses would be made available. Little data or analyses would be centrally located—GAIN envisions creating a distributed, worldwide virtual database.

GAIN has developed instructive approaches to overcome information-sharing barriers. First, GAIN has several procedures designed to protect sensitive material. GAIN participants share little or no raw data, and sharing is completely voluntary. To avoid embarrassment, aviation companies strip information submitted to GAIN of all identifiers so that it cannot be traced back to the source. The FAA has also encouraged businesses and foreign nations to adopt a climate receptive to reporting problems in order to avoid "shooting the messengers." Sensitive information is protected from FOIA requests by statute and Exemption (b)(3).

Second, there are concerns that sensitive information could be disclosed during accident litigation, particularly during the discovery phase. It is unlikely that legislation could be crafted to protect information disclosures from litigation. However, since GAIN envisions using de-identified material only, there is some protection for aviation carriers from litigation discovery.

Finally, there are significant factors motivating the aviation industry to participate in GAIN. Given that accidents could affect any carrier, it is in the carriers' best interest to share information and analyses that could prevent accidents. Lower accident rates should decrease insurance rates, thus providing a strong financial incentive for all carriers. *Not* participating in GAIN may have a negative impact on a company's image if the public perceives it is not as safety conscious as its competitors. Finally, due diligence issues arise if an aviation company does not participate in GAIN and consequently lacks safety information that it would otherwise have. These factors create a strong case for full, voluntary participation in GAIN.

GAIN faces many of the information sharing barriers reviewed in the previous chapter. GAIN seeks to protect sensitive information by only accepting voluntarily submitted information, avoiding raw data, and de-identifying submitted information. FOIA Exemptions (b)(3) and (b)(4) protect sensitive material from release. There are strong incentives for an aviation company to participate in GAIN. Finally, the primary reason the FAA proposed GAIN is an imperative common to all aviation companies: reduce aviation accidents to zero.

Summary

Numerous organizations successfully share sensitive information between the government and private sector. This section examined four such organizations with a particular focus on how each has overcome various barriers to information sharing. One particular feature of each entity that cannot be overemphasized is trust—voluntary information sharing and partnership can only exist in an atmosphere of trust. Building the proper environment for trust to flourish is not easy and requires considerable investments in time and effort from the government and private sector alike. However, given the benefits that information sharing has to offer, nurturing trust is well worth the investment.

The lessons learned from the model organizations in this chapter point to next steps that the government and private sector should undertake jointly. The next section explores these steps and outlines associated policy recommendations.

POLICY RECOMMENDATIONS

> *There are two ways to help people appreciate the magnitude of electronic and cyber threats. One learns by being burned, and inevitably much public appreciation will come the hard*

> *way. The other way is to learn through information and warnings.*[100]

Given the overall importance of information exchanges in risk reduction and management programs, the government and private sector should cooperate closely to develop an information sharing mechanism. The following paragraphs recommend specific policy actions to help the government chart a path forward.

1. Engage the private sector from the onset. By definition, the private sector is a partner in any information-sharing mechanism. As such, the government must engage the private sector from the onset in any design of an information-sharing mechanism. A frequently heard complaint regarding government's critical infrastructure protection program is that the government *has not* been sufficiently proactive with the private sector to foster the necessary partnership.[101] The private sector does not want a government-mandated solution thrust upon it; such an approach will do substantial damage and hinder, if not outright halt, any attempt to build a mutually beneficial partnership. Instead, actively engaging the private sector as a full partner will help build the trust vital to the operation of an information-sharing mechanism.
2. Determine information requirements. The specific types of information that the government and private sector should share have not been clearly delineated. As the NCC's tabletop exercise demonstrated, information requirements vary among the military, intelligence, law enforcement, and private sector communities, which subsequently complicates the problem. Furthermore, information requirements vary by level in the government or corporate hierarchy. Nevertheless, defining *what* information the

government and private sector need to reduce risks and *what* each party is willing to share—particularly given the barriers—are essential preliminary questions to answer.[102] Closely related are the issues of who should be involved and how the information flows should be controlled. Once these preliminary questions are answered, the government and private sector can develop detailed formal guidance and procedures for reportable information.

3. <u>Release selected threat, vulnerability, and risk information to key members of the private sector</u>. The private sector has made it clear that it does not view the threat to be as serious as the government states. NSTAC noted "increased awareness is essential in narrowing the gap between industry and Government with regard to the perceived threat to the infrastructures. *Industry is not convinced there is a need to allocate additional resources toward protection*."[103] Releasing key information to the appropriate private sector officials, such as chief executive officers and chief technology officers, will not only fulfill this awareness function but will go a long way towards obtaining private sector buy-in. Clearly, issues of classified information must be addressed, with one-time releases to cleared industry officials as a potential solution. Until industry is convinced that it faces clear, persistent, and substantial threats and risks, making the business case for information sharing will be difficult at best and impossible at worse.
4. <u>Address the FOIA and antitrust barriers first</u>. Industry has indicated that FOIA and antitrust concerns are show-stoppers. In partnership with the private sector, the government should address these two barriers first. As noted earlier, the government has already held a conference on the FOIA issue that included private

sector participation. At the conference, DOJ took an action to examine potential legislation for a (b)(3) exemption. It cannot be overemphasized that DOJ needs to work with the private sector in drafting the statute. Using the experience of the NCC as guidance, the government should ensure that DOJ's Antitrust Division, the Federal Trade Commission, and FCC play active roles in crafting solutions to antitrust issues. Additional workshops on FOIA and antitrust issues, in which government and private sector legal experts explore in detail the issues and develop mutually acceptable solutions, are steps in the right direction.

5. Build up slowly. Developing a trusted environment takes time—it cannot be mandated by government policy or law. Taking a series of smaller steps toward the goal of an information-sharing entity, such as a series of pilot projects that build upon each other, may be more effective than a giant leap toward the final entity. In any case, patience will be essential.
6. Build on existing entities. NCC, the NSIEs and CERT/CC are existing, successful information-sharing mechanisms. These organizations, singly or collectively, could provide a base for an expanded information-sharing mission, as in the case with NCC's IAW pilot project. Furthermore, these organizations have already established the trust necessary to encourage information sharing. They also have experience in overcoming information-sharing barriers, and have developed internal procedures and policies to resolve associated issues. Evolving an existing structure toward a broader information sharing or IAW mission offers substantial advantages over establishing a new structure from the ground up.
7. Consider pilot projects. Pilot projects may provide the necessary experience and develop the requisite trust. The government may

wish to consider a government-only pilot project in which government information is submitted, analyzed, and disseminated to participating departments and agencies. The private sector could initially observe the pilot project, with an option to fully join at a later date. A pilot project that provides substantial benefits or shows substantial returns on investment could motivate the private sector to partner with the government. The primary drawback to a government-only pilot project is that the overwhelming majority of government information and communications traffic rides on privately owned information infrastructure assets. Hence, a government-only pilot would not benefit from crucial private sector information and inputs.

CONCLUSIONS

> *Although infrastructure failures could be catastrophic from a national security perspective, it is equally relevant to indicate that those same failures and outages would also have profound implications for businesses. Furthermore, as Government increasingly relies on the private sector and its assets, failures in commercial infrastructures could seriously affect its ability to meet its NS/EP requirements.*[104]

The United States faces a growing information threat and increased risks in the coming years. Given the impossibility of completely protecting the DII and NII, the military must develop a means to reduce risks posed by electronic intrusions and attacks to acceptable levels. Given the military's heavy use of commercial information infrastructure assets, it is crucial that the defense establishment share information on electronic intrusions and attacks with the private sector. Furthermore, the military cannot share information in isolation from the rest of government—a military-private sector information exchange program must be an integral element of a broader government-private sector effort.

The government and private sector face substantial information-sharing barriers. A number of successful information-sharing forums operate today, which provides good reason to believe that the government and private sector can find mutually acceptable solutions to the barriers. The existing forums serve as models, providing valuable lessons learned that could be incorporated in an information-sharing forum on electronic intrusions and attacks. The key, though, lies in close cooperation between the government and private sector from the onset. Cooperation, in which the government considers the private sector's concerns and positions and actively engages the private sector in the development of solutions, is a prerequisite to the establishment of a successful sharing mechanism. Building the necessary trust will take time and substantial effort on the part of both the government and private sector.

Developing a meaningful, successful information-sharing mechanism is essential if the government and private sector are to prevail against increasingly sophisticated information threats in the coming years. Given the magnitude of the challenges and the consequences of failure, moving forward with a constructive dialog is the wisest path for both to follow.

[1] Testimony of John Deutch, Director of Central Intelligence, before the Senate Subcommittee on Governmental Operations, 22 June 1996.

[2] President, *Critical Infrastructure Protection*, Presidential Decision Direction-63 (22 May 1998). Available on the Internet at www.ciao.ncr.gov/resources.html (as of 7 September 1999).

[3] Office of the Manager, National Communications System, *The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications: An Awareness Document,* 3d ed. (Arlington, VA: Office of the Manager, National Communications System, March 1999), 53-54. Available on the

Internet at www.ncs.gov/n5_hp/n5_ia_hp/GovPub.html (as of 25 September 1999).

4. Office of the Manager, National Communications System, *An Assessment of the Risk to the Security of Public Networks* (Arlington, VA: Office of the Manager, National Communications System, December 1995), 14.

5. Office of the Manager, National Communications System, *Electronic Intrusion Threat*, 3.

6. Ibid., ES-4.

7. Defense Science Board Task Force on Information Warfare-Defense, *Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)* (Washington, DC: Office of the Undersecretary of Defense for Acquisition and Technology, November 1996), 2-15. This reference describes the procedure by which DISA estimated the number of possible intrusions into DoD information systems.

8. Colonel Gregory Frick, "Warfare in the Information Age," DoD briefing to the National Security Telecommunications Advisory Committee, Industrial Executive Subcommittee (McLean, VA, 22 July 1999).

9. Terrill D. Maynard, *Year 2000 Computer Remediation: Assessing Risk Levels in Foreign Outsourcing* (Washington, DC: National Infrastructure Protection Center, 1999). Available on the Internet at www.sans.org/newlook/resources/Y2K.htm (as of 25 September 1999).

10. Joint Staff, *Information Assurance: Legal, Regulatory, Policy and Organization Considerations*, 3d ed. (Washington, DC: Joint Staff, 17 September 1997), 7-7.

11. Note that these are *only* the incidents reported to CERT/CC, not the sum total of *all* incidents for a given year. Many incidents go unreported for various reasons. CERT/CC statistics, available on the Internet at www.cert.org/stts/cert_stat.html (as of 6 September 1999).

12. Office of the Manager, National Communications System, *Electronic Intrusion Threat*, 21.

13. Detection of malicious code received emphasis in the White House Office of Science and Technology Policy's (OSTP) research and development agenda for critical infrastructure protection. Critical Infrastructure Protection R&D Interagency Working Group, *Toward a*

Federal R&D Agenda in Critical Infrastructure Protection, unpublished report (November 1998). Additionally, during a joint OSTP-Department of Energy workshop on intrusion detection, malicious code, and insider threats (22-23 February 1999), there was agreement that detecting hostile code embedded in software products is an exceptionally difficult problem.

14. Maynard, *Year 2000 Computer Remediation*.

15. Defense Science Board Task Force on Information Warfare-Defense, *Report*, 2-12.

16. Office of the Manager, National Communications System, *Electronic Intrusion Threat*. In particular, see the Executive Summary for a review of the key trends.

17. Eligible Receiver was a DoD exercise in 1997. The "red team" used only hacker tools available on the Internet and was restrained by several rules of engagement. Nevertheless, the team "inflicted" substantial damage and demonstrated weaknesses in DoD computer security. Solar Sunrise was a series of intrusion events into military computer networks. The hackers turned out to be a pair of California teenagers assisted by an Israeli. However, the intrusions occurred during a buildup of U.S. forces in Southwest Asia for a possible attack against Iraq. Initially, it was not known if the attacks were part of a concerted information warfare campaign against the U.S. in conjunction with preparations for hostilities. During the summer of 1999, a series of attacks against federal government web sites occurred (including the White House, Department of the Interior, Department of Energy, and the Federal Bureau of Investigation). Some of the attacks were apparently in retaliation for the accidental U.S. bombing of the Chinese embassy in Belgrade during the Kosovo conflict.

18. Office of the Manager, National Communications System, *Electronic Intrusion Threat*, 4-5.

19. Ibid., ES-1.

20. Defense Science Board Task Force on Information Warfare-Defense, *Report*, 2-9.

21. Ibid., 2-14.

22. National Security Telecommunications Advisory Committee, Network Group, Widespread Outage Subgroup, *Report on the Likelihood of a Widespread Telecommunications Outage* (Washington,

DC: National Security Telecommunications Advisory Committee, December 1997), 4.

23. Ibid., 1.

24. Ibid., 5.

25. Borrowing a concept from statistics, one should examine not just the *probability* of a serious attack but also the *expectation value* of the associated national security, economic security, and societal costs. Note that rare events with high societal costs and frequent events with low costs both yield appreciable expectation values. Of perhaps greater concern here are those rare events with high societal costs.

26. Joint Staff, *JP 3-13, Joint Doctrine for Information Operations* (Washington, DC: Joint Staff, 9 October 1998), I-9. The publication further notes that "**Information, information systems, and information-based processes** (such as C2, communications, weapons systems) used by US military forces will be protected relative to the value of the information they contain and the risks associated with their compromise or loss of access. The value of information may change in relation to the objectives during peace, crisis, conflict, or postconflict, as well as during the various phases of an operation." (Emphasis in original.) Implicit in this directive is determining the level of each system's risk and appropriate protection levels. I-5.

27. The report of the President's Commission on Critical Infrastructure Protection contains an extensive discussion of risks to the nation's critical infrastructures and policy recommendations to protect them. These infrastructures include the electric power grid, oil and natural gas production and storage, transportation networks, banking and finance systems, water systems, and information and communication networks. President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, DC: President's Commission on Critical Infrastructure Protection, October 1997).

28. Office of the Chairman of the Joint Chiefs of Staff, *Joint Vision 2010* (Washington, DC: Joint Chiefs of Staff, 1997), 16. Emphasis in original.

29. Ibid., 19.

30. Air Force doctrine defines information superiority as "the ability to collect, control, exploit, and defend information while denying an adversary the ability to do the same and, like air and space superiority,

includes gaining control over the information realm and fully exploiting military information functions." Headquarters Air Force Doctrine Center, *Air Force Doctrine Document 1: Air Force Basic Doctrine* (Maxwell AFB, AL: Headquarters Air Force Doctrine Center, September 1997), 31-32.

31. Headquarters Air Force Doctrine Center, *Air Force Doctrine Document 2-5: Information Operations* (Maxwell AFB, AL: Headquarters Air Force Doctrine Center, 5 August 1998), 2, 15.

32. Joint Staff, *JP 3-13*, x, I-12, I-13, III-12.

33. John R. Boyd, "A Discourse on Winning and Losing," unpublished briefings and essays, Document No. MU 43947 (Maxwell AFB: Air University Library, August 1987). Boyd introduces his concept on page 5 of Chapter 1, "Patterns of Conflict," and develops it with historical examples.

34. Headquarters Air Force Doctrine Center, *Air Force Doctrine Document 2-5*, 1. Emphasis in original.

35. Network Reliability and Interoperability Council, *Network Interoperability: The Key to Competition* (Washington, DC: Network Reliability and Interoperability Council, 15 July 1997), 110-111.

36. Office of the Manager, National Communications System, *Electronic Intrusion Threat*, ES-2.

37. The Defense Science Board saw no evidence that existing components or systems under design could provide a completely hardened infrastructure. Defense Science Board Task Force on Information Warfare- Defense, *Report*, 2-7. More recently, the Committee on Information Systems Trustworthiness, National Research Council, examined *inter alia* the issue of developing trustworthy networks from untrustworthy components and provided extensive policy and research recommendations. National Research Council, *Trust in Cyberspace* (Washington, DC: National Academy Press, 1999).

38. Joint Staff, *JP 3-13*, II-12, II-13.

39. President, *Critical Infrastructure Protection*.

40. President's Commission, *Critical Foundations*, 27-33.

41. NSTAC has often cited the importance of information sharing. See, for example, National Security Telecommunications Advisory

Committee, Network Group, Intrusion Detection Subgroup, *Report on the NS/EP Implications of Intrusion Detection Technology Research and Development* (Washington, DC: National Security Telecommunications Advisory Committee, December 1997), 30, 36; National Security Telecommunications Advisory Committee, Operations Support Group Report, *NSTAC XX Report* (Washington, DC: National Security Telecommunications Advisory Committee, December 1997), 3-4.; National Security Telecommunications Advisory Committee, National Coordination Center for Telecommunications Vision Subgroup Report, *NSTAC XX Report* (Washington, DC: National Security Telecommunications Advisory Committee, December 1997).

42. See, for example, National Security Telecommunications Advisory Committee, Information Assurance Task Force, *Electric Power Information Assurance Risk Assessment* (Washington, DC: National Security Telecommunications Advisory Committee, March 1997); National Security Telecommunications Advisory Committee, Information Infrastructure Group, *Financial Services Risk Assessment Report* (Washington, DC: National Security Telecommunications Advisory Committee, December 1997); National Security Telecommunications Advisory Committee, Information Infrastructure Group, *Interim Transportation Information Risk Assessment Report* (Washington, DC: National Security Telecommunications Advisory Committee, December 1997).

43. National Security Telecommunications Advisory Committee, National Coordination Center for Telecommunications Vision Subgroup Report, *NSTAC XX Report*, 4.

44. National Coordinating Center for Telecommunications, *NCC Vision Subgroup Tabletop Exercise After-Action Report* (Washington, DC: OMNCS, 13 August 1997).

45. During the drafting of PDD-63, law enforcement officials emphasized the need for the private sector and government to rapidly provide raw, unfiltered intrusion information directly to NIPC. Speed is of the essence in order to preserve perishable case information. From the author's personal observations.

46. Available on the Internet at www.cert.org/ftp/incident_reporting_form (as of 7 September 1999).

47. Available on the Internet at www.cert.org/ftp/vul_reporting_form (as of 7 September 1999).

[48] Available on the Internet at www.cert.org/ftp/response_team_IRF.txt (as of 7 September 1999).

[49] National Security Telecommunications Advisory Committee, National Coordination Center for Telecommunications Vision Subgroup Report, *NSTAC XX Report*, D-5.

[50] During the joint OSTP-Federal Bureau of Investigation (FBI) Workshop on Infrastructure Interdependencies, a number of participants stressed that the government must be more forthcoming with threat and vulnerability information before the private sector will be willing to justify undertaking additional security measures. In particular, one private sector participant stated that his organization would need threat or vulnerability information such as "there is a threat that will intrude upon your system tomorrow by exploiting this specific vulnerability." Author's notes, Joint OSTP-FBI Workshop on Infrastructure Interdependencies, Washington, DC, August 12-13, 1999.

[51] Potomac Institute for Policy Studies, *Proceedings Report: Seminar on Cyber-Terrorism and Information Warfare: Threats and Responses* (Washington, DC: Potomac Institute for Policy Studies, 17 April 1998), 24.

[52] Defense Science Board Task Force on Information Warfare-Defense, *Report*, 6-9.

[53] Private sector and government participants at a White House conference on information sharing pointed to the FOIA issue as a show-stopper for information exchanges. White House Conference, "Sharing Critical Infrastructure Information: The Freedom of Information Act," White House Conference Center, Washington, DC, 21 July 1999 (hereafter referred to as FOIA Conference).

[54] Even though it shares sensitive telecommunications information, the NCC has not yet received a FOIA request. NSTAC's Legislative and Regulatory Group noted that "should public awareness of NCC operations increase, FOIA requests for records may become a concern for participating companies. Participants may be reluctant to share information with the NCC if the NCC is unable to ensure that such records qualify for exemption and can be withheld upon request…To date, the NCC has not been the subject of any FOIA requests, but the concern exists that FOIA could eventually become a barrier to sharing information." National Security Telecommunications Advisory Committee, Legislative and Regulatory Group, *Telecommunications*

Outage and Intrusion Information Sharing Report (Washington, DC: National Security Telecommunications Advisory Committee, June 1999), 26 and Footnote 13.

55. Wayne Madsen, *Critical Infrastructure Protection and the Endangerment of Civil Liberties* (Washington, DC: Electronic Privacy Information Center, October 1998), 17. Available on the Internet at www.epic.org/security/infowar/epic-cip.html (as of 12 September 1999). EPIC is a public interest research organization, established to "focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values."

56. However, this viewpoint is easily countered by asserting that the private sector, once cognizant of significant threats and vulnerabilities through a confidential (e.g., nonpublic) information sharing mechanism, will take security measures commensurate with the risks—and avoid public embarrassment or loss of confidence at the same time.

57. 5 U.S.C. § 552(b)(3).

58. Note that § 4(f)(3)(A) of Public Law 105-27/112 Stat. 2386, "Year 2000 Readiness and Disclosure Act," is an example of a statute that provides protection against the FOIA for information sharing related to information systems.

59. At the FOIA Conference, the Department of Justice took an action to begin drafting such legislation.

60. Federal Aviation Administration, Office of System Safety, *Aviation Safety Information: Four Potential Problems; Four Proposed Solutions* (Washington, DC: Federal Aviation Administration, January 1998), 3. Available on the Internet at nasdac.faa.gov/GAIN/Problems_Solutions/INFOPROB.htm (as of 12 September 1999).

61. Participant comments during the FOIA Conference.

62. FOIA Conference participants generally believed that the FOIA issue can be resolved, albeit with some effort.

63. President's Commission on Critical Infrastructure Protection, *Legal Impediments to Information Sharing: A "Legal Foundations" Study* (Washington, DC: President's Commission on Critical Infrastructure Protection, 1997), 24.

64. Office of the Manager, National Communications System, *NCS LEGAL LANDSCAPE: Presidential Decision Directive 63 and Beyond*, unpublished briefing charts (December 1998).

65. Ibid., p. 29F.

66. In this section, "confidential" information refers to trade secrets, proprietary information, personal data, etc. It does not refer to national security information classified at the CONFIDENTIAL level.

67. President's Commission on Critical Infrastructure Protection, *Information Sharing Models: A "Legal Foundations" Special Study* (Washington, DC: President's Commission on Critical Infrastructure Protection, 1997), 26.

68. Madsen, *Endangerment*, 3.

69. Potomac Institute for Policy Studies, *Proceedings Report*, 32.

70. FIDNET is a National Security Council proposal to monitor federal computer systems for electronic intrusions. As currently planned, FIDNET is designed strictly for federal computers. However, in the future the private sector will be invited to participate in the intrusion detection system. See "FIDNET Under Review," *Wired News*, 29 July 1999, available on the Internet at www.wired.com/news/politics/story/21001.html (as of 26 September 1999); Declan McCullagh, "Surveillance Network Draws Fire," *Wired News*, 29 July 1999, available on the Internet at www.wired.com/news/politics/story/20994.html (as of 26 September 1999); Robert O'Harrow Jr., "Computer Security Proposal is Revised," *Washington Post*, 22 September 1999.

71. Office of Management and Budget, *Management of Federal Information Resources*, Circular No. A-130, revised (Washington, DC: OMB, February 1996), 5.

72. Ibid., 6.

73. President, *Critical Infrastructure Protection*, 3.

74. President's Commission, *Critical Foundations*, 87.

75. For example, industry will be more reluctant to provide information if regulators have access to it. National Security Telecommunications Advisory Committee, Information Infrastructure Group, *Cyber Crime Point Paper* (Washington, DC: National Security Telecommunications Advisory Committee, 21 October 1997), 3.

76. President's Commission on Critical Infrastructure Protection, *Legal Impediments*, 3-5.

77. Office of the Manager, National Communications System, *NCS LEGAL LANDSCAPE*, 29.

78. President's Commission on Critical Infrastructure Protection, *Legal Impediments*, 7.

79. "Establishing and Maintaining the Confidentiality of Critical Infrastructure Information," Security Policy Board briefing to the Critical Infrastructure Assurance Office (Washington, DC, 2 December 1999). Emphasis in original.

80. Alternatively, "protectable critical infrastructure information" could be defined broadly enough to include the information infrastructure, thereby precluding the need for two separate but virtually identical systems.

81. National Coordinating Center for Telecommunications, *Tabletop Exercise After-Action Report*, 6.

82. Office of the Manager, National Communications System, *Electronic Intrusion Threat*, 63.

83. President's Commission, *Critical Foundations*, 31.

84. This figure relates to information clearinghouses only; when other forms of sharing mechanisms are considered, the total is much higher. President's Commission on Critical Infrastructure Protection, *Information Sharing Models*, 7.

85. National Security Telecommunications Advisory Committee, Legislative and Regulatory Group, *Telecommunications Outage.*

86. Office of the Manager, National Communications System, *Electronic Intrusion Threat*, 60.

87. National Coordination Center for Telecommunications, *Operational Guidelines* (1984), 2.

88. National Security Telecommunications Advisory Committee, Legislative and Regulatory Group, *Telecommunications Outage*, 17.

89. National Coordination Center for Telecommunications, *Operational Guidelines*, 15.

90. National Security Telecommunications Advisory Committee, Legislative and Regulatory Group, *Telecommunications Outage*, 27.

91. William Baxter, Assistant Attorney General, DOJ Antitrust Division, to Lieutenant General William Hilsman, Manager, National Communications System, 1 June 1983, file copy, Critical Infrastructure Assurance Office, Washington, DC.

92. William Baxter, Assistant Attorney General, DOJ Antitrust Division, to Lieutenant General Winston D. Powers, Manager, National Communications System, 14 November 1983, file copy, Critical Infrastructure Assurance Office, Washington, DC.

93. Baxter (14 November 1983).

94. Mimi Weyforth Dawson, FCC Defense Commission, to Lieutenant General Winston D. Powers, Manager, National Communications System, 1 December 1983, file copy, Critical Infrastructure Assurance Office, Washington, DC.

95. National Security Telecommunications Advisory Committee, Legislative and Regulatory Group, *Telecommunications Outage*, 20-22.

96. CERT® Coordination Center, *Meet the CERT® Coordination Center*, Appendix A. Available on the Internet at www.cert.org/meet_cert/meetcertcc.html (as of 6 September 1999).

97. Although it could be argued that releasing *any* vulnerability information assists the hacker community, CERT/CC's release of vulnerability and patch information simultaneously overcomes this criticism. It is incumbent, of course, upon system administrators to be aware of, obtain, and install patches, thereby eliminating vulnerabilities.

98. CERT® Coordination Center, *Meet the CERT® Coordination Center*.

99. A considerable volume of information on GAIN is available at the GAIN web site, www.gainweb.org.

100. Stephan Lukasic, quoted in National Security Telecommunications Advisory Committee, Information Infrastructure and Operations Support Groups, *Information Assurance: A Joint Report* (Washington, DC: National Security Telecommunications Advisory Committee, December 1997), 15.

101. Author's personal observations. This issue was frequently raised during the drafting of PDD-63.

102. A focused tabletop exercise, building on the NSTAC NCC Vision Subgroup's 1997 exercise, would be an excellent means to begin answering these key questions.

103. National Security Telecommunications Advisory Committee, Information Infrastructure and Operations Support Groups, *Information Assurance*, 16. Emphasis added.

104. National Security Telecommunications Advisory Committee, Network Group, Intrusion Detection Subgroup, *NS/EP Implications*, 8.